UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/611,809	07/07/2000	David K. Chin	2875.0640001	6867

26111 7590 07/11/2007

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
07/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Advisory Action Before the Filing of an Appeal Brief	Application No.	Applicant(s)	
	09/611,809	CHIN ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 25 June 2007 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☐ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☒ The period for reply expires 3 months from the mailing date of the final rejection.
   b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: 1,2,4,7-9,12 and 14-30.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

Continuation of 11. does NOT place the application in condition for allowance because: Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged. Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 U.S.C. 119(e) as follows:
The later-filed application must be an application for a patent for an invention which is also disclosed in the prior application (the parent or original nonprovisional application or provisional application). The disclosure of the invention in the parent application and in the later-filed application must be sufficient to comply with the requirements of the first paragraph of 35 U.S.C. 112. See Transco Products, Inc. v. Performance Contracting, Inc., 38 F.3d 551, 32 USPQ2d 1077 (Fed. Cir. 1994).
The disclosure of the prior-filed application, Application No. 60/142,891, fails to provide adequate support or enablement in the manner provided by the first paragraph of 35 U.S.C. 112 for one or more claims of this application. None of the drawings of the later-filed application is identical to the drawing of the prior-filed application. In addition, at least the following claims of the later-filed application do not have support or enablement in the prior-filed application: Claim 1 recites,
A server to perform computations to establish a secure
network session, comprising of: a system memory; and a processing unit coupled to said system memory via a system bus, the processing unit obtains values for a modulus N, a private key d, and a cipher text C sent by a client and calculates a value for clear text M for each request for a secure network session made to the server by the client, the processing unit includes:
an execution unit, coupled to a decode unit, configured to execute arithmetic instructions to perform product and square operations, the execution unit including at least one adder and at least two multipliers configurable to perform specified multiplication operations in parallel and configurable to perform specified multiplication and addition operations in parallel;
the decode unit to receive requests for establishing a secure network session from the client, the decode unit configured to determine if a square operation or a product operation needs to be performed on an operand, the decode unit further configured to issue the arithmetic instructions to the execution unit so that the execution unit performs specified multiplication and addition operations in parallel and performs specified multiplication operations in parallel while performing either the square or product operation.
Claim 21 recites
A method to establish a secure network session, comprising the steps of:
sending an encrypted message to a server using a public key; decrypting said encrypted message by the server using a private key; and generating a symmetrical key to encrypt/decrypt messages transmitted and received between a client and the server, wherein generation of the public key, the private key, and/or the symmetrical key further comprises computation of a modular exponentiation operation using the Montgomery method, wherein said Montgomery method further comprises:
receiving, by a decode unit, a request to perform a modular operation;
determining, by the decode unit, whether a Montgomery square operation or a Montgomery product operation is to be performed;
issuing, by the decode unit, a first instruction to perform a Montgomery square operation;
issuing, by the decode unit, a second instruction to perform a Montgomery product operation;
performing, by an execution unit, simultaneous multiplication operations in response to at least one of the first instruction and the second instruction; and
performing, by the execution unit, simultaneous multiplication and addition operations in response to at least one of the first instruction and the second instruction.
Claim 22 recites
A method to establish a secure network session, comprising the steps of:
sending an encrypted message to a server using a public key; decrypting said encrypted message by said server using a private key; and generating a symmetrical key to encrypt/decrypt messages transmitted and received between a client and said server, wherein said public key, said private key, and/or said symmetrical key further comprises computation of a modular exponentiation operation using the Montgomery method, wherein said Montgomery method further comprises:
determining, by a decode unit, whether to perform a Montgomery square operation or a Montgomery product operation;
issuing, by the decode unit, a first set of instructions for an execution unit to
perform the Montgomery square operation, the first set of instructions comprising; a first instruction to perform simultaneous multiplication operations; and
a second instruction to perform simultaneous multiplication and addition operations; and
issuing, by the decode unit, a second set of instructions for an execution unit to
perform the Montgomery product operation, the second set of instructions comprising: a third instruction to perform simultaneous multiplication operations;
a fourth instruction to perform simultaneous multiplication and addition operations; and
a fifth instruction to perform simultaneous multiplication and addition operations.

Therefore, applicant's arguments regarding Shaham not prior art for the instant application is not persuasive. The request for reconsideration has been considered but does not place the application in condition for allowance. .

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

7/10/07